REMARKS/ARGUMENTS

Favorable reconsideration of this application as presently amended and in light of the following discussion is respectfully requested.

Claims 1-20 are pending in the present application. Claims 1, 2, 7, 8, 13 and 14 are amended by way of the present amendment.

Support for the amendments to the claims can be found, at least, in Figures 2, 3, 4 and 8. Thus, no new matter is added.

In the outstanding Office Action, Claims 1-4, 6-10 and 12-20 were rejected under 35 U.S.C. §102(b) as anticipated by Shurts (U.S. Pat. No. 5,572,673); and Claims 5 and 11 were rejected under 35 U.S.C. §103(a) as unpatentable over Shurts in view of Timmer (U.S. Pat. Pub. No. 2002/0107895).

Before turning to the outstanding prior art rejections, it is believed that a brief review of the present invention would be helpful.

In a non-limiting example, illustrated in Figure 10 two users, "A" and "B", are able to exchange information and foster human relations using the present invention. For instance, the information communication device "A" may have visited a movie theatre earlier in the week. During this visit, the name of the movie and the location of the theatre are entered into the metadata storage unit of the user's information communication device "A" automatically by a radio transmitter located at the theatre. Because the user "A" has programmed the security table of his information communication device as is shown in Figure 5, the movie theatre transmitter is able to deliver metadata to the information communication device of user "A" and store it in a partition of the device corresponding to security level 1. User "B" may have also watched the same movie at a different location two weeks ago and metadata relating to the movie was also entered into security level 1 of user "B"s information communication device. As shown in Figure 10, when user "A" and user "B" both enter the

room which includes device "C", device "C" scans the publicly available partitions (corresponding to security level 1 for instance) of each information communication device. The device "C" then matches the movie seen by user "A" and "B" and sends a notification to both matched users letting user "B" know that user "A" has seen the movie and notifying "A" that user "B" has seen the movie. This allows users "A" and "B" to know which users they have things in common with such as they have been to the same parties or they have seen the same movies.

With respect to the rejection of Claims 1-4, 6-10 and 12-20 under 35 U.S.C. § 102(b) as anticipated by Shurts, Applicant respectfully traverses this rejection. Amended Claim 1 will be the first claim discussed and it recites, in part,

> a radio communication unit which transmits and receives radio communication data;
> a metadata storage unit which stores metadata relating to a user of the communication device; and
> a central control unit which manages the storage of metadata in said metadata storage unit, wherein said central control unit
> partitions said metadata storage unit by security level and category,
> stores metadata received through said radio communication unit in a corresponding partition of the metadata storage unit based on matching the received metadata with a security level and/or category predetermined by the user, and
> supplies, in response to an external access request, metadata from the metadata storage unit that matches a security level available to the external access request or that matches the security level available and category requested.

Claim 7 recites similar features.

Shurts describes a database management system which gives users temporary or controlled access to objects having sensitivities that do not match the access level of the user. For instance a user with an unclassified status would be able to upload unclassified data to a

classified database but would not be able to access any other classified data. Further Shurts describes that metadata can be included in tables (such as table ID or audit settings).

However, Shurts does not teach or suggest a metadata storage unit which stores metadata relating to a user of the communication device.

Further, Shurts does not teach or suggest storing metadata received through a radio communication unit in a corresponding partition of a metadata storage unit based on matching the received metadata with a security level and/or category predetermined by the user.

In other words, Shurts merely describes a secure database that is stored on a server 52 and client PCs 54 are able to access certain objects in the database based on the access rights of the user and the sensitivity level of the object. Further, in Shurts, the metadata is attached to the databases and is used to determine the sensitivity of objects (confidential, top secret, etc) in the database. Shurts does not describe storing metadata relating to a user of an information communication device on the information communication device itself. Further, Shurts does not describe or suggest storing metadata in a corresponding partition of the metadata storage unit based on matching the received metadata with a security level and/or category predetermined by the user.

Thus, Shurts does not provide the advantage of the claimed invention in that human relations are fostered by the use of the claimed information communication device.

Thus as Shurts does not describe all of the features recited in Claim 1, Claim 1 and similarly Claim 7 patentably distinguishes over Shurts.

In addition, the further cited Timmer reference does not cure the above noted deficiencies of Shurts with regard to Claims 1 and 7.

Accordingly, Applicants respectfully submit that Claims 1 and 7 and claims depending therefrom patentable distinguish over Shurts and Timmer individually or in combination.

Further with regard to Claims 2 and 8 Applicants respectfully submit that the features recited therein are not taught or suggested by Shurts.

The outstanding Action states in section 3.2, "Shurts is directed to a secured database system and the purpose of databases is storing linked pieces of information such as the user, its visits and the visited place." Applicants respectfully traverse that just because Shurts describes a database that the features recited in Claims 2 and 8 are anticipated by Shurts.

Claim 1 recites that "said metadata is information in the form of metadata, equivalent to a log providing information on locations visited by the user." Although this metadata may be able to be stored in a database, Shurts does not describe metadata which includes a log which provides information on locations visited by the user. Further Shurts actually teaches away from the features recited in Claims 2 and 8. In Shurts, the metadata is used to identify objects in a database not as the objects of the database itself. Further, Shurts makes no mention of "locations visited by the user."

Accordingly, Applicants respectfully submit that Claims 2 and 8 patentably distinguish over Shurts.

Turning now to the rejection of Claim 13 under 35 U.S.C. §102(e) as anticipated by Shurts.

Claim 13 recites, in part,

> a metadata transmitting means which provides user terminals with metadata that corresponds to a security level and at least one category at different locations in the physical world;
>
> a metadata acquiring means which retrieves metadata that matches the security level and category of the request from user terminals;

> a matching means which performs matching among pieces of metadata acquired from two or more user terminals; and
>
> a result of matching presenting means which presents the result of the matching to the user terminals from which the matched pieces of metadata was acquired.

As noted above, Shurts merely describes a secure database and the method of authentication. Shurts clearly does not describe or suggest a metadata transmitting means which provides user terminals with metadata that corresponds to a security level and at least one category at different locations in the physical world.

Further, Shurts also clearly does not describe acquiring metadata from user terminals, matching the metadata and presenting the match to the user terminals from which the metadata was acquired.

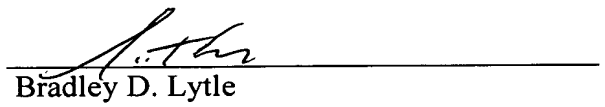
In other words, Shurts merely describes a database but not describe the method as recited in Claim 13. Thus, Shurts does not provide the advantageous advantages of the present invention of furthering physical world human relations through use of virtual world technology.

Therefore, Applicants respectfully submit that Claim 13 and claims depending therefrom patentably distinguish over the cited Shurts reference.

Consequently, in view of the present amendment, no further issues are believed to be outstanding in the present application, and the present application is believed to be in condition for formal Allowance.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.



Bradley D. Lytle
Attorney of Record
Registration No. 40,073

Scott A. McKeown
Registration No. 42,866

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 06/04)

I:\ATTY\JL\240894US\240894US_AM.DOC